



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,370	07/31/2003	Stuart S. Kreitzer	CE11296JEM	2130
24273	7590	02/27/2006	EXAMINER	
MOTOROLA, INC INTELLECTUAL PROPERTY SECTION LAW DEPT 8000 WEST SUNRISE BLVD FT LAUDERDAL, FL 33322			KLIMACH, PAULA W	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 02/27/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/631,370

Applicant(s)

KREITZER, STUART S.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-12 and 14-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-12 and 14-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/28/06 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 7, 10, 14, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki (5,390,252) in view of Whelan et al (6,965,674 B2)

In reference to claims 1 and 14, Suzuki discloses a system and method of establishing secure communications in a multi-mode portable communication device, comprising the steps of: establishing a symmetric traffic key between the multi-mode portable communication device and a second portable communication device in a first mode of communication (Fig. 3); switching to at least a second mode of communication (column 5 lines 38-45); and sharing the symmetric traffic key between the multi-mode portable communication device and the second portable communication device (column 5 line 60 to column 6 line 12).

Suzuki does not expressly disclose storing the traffic key in a recent call list that reflects recent communications between the portable communication device and the second portable communication device.

Whelan discloses a system wherein the traffic key is stored in a recent call list that reflects recent communication between the portable communication device and a second portable communication device (column 5 lines 30-33; column 10 lines 19-42; Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the traffic key in a recent call list as in the system of Whelan in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because it would make it impractical for a hacker to gather sufficient network traffic using any one WEP key to decrypt that key (Whelan column 7 lines 54-65).

In reference to claim 7, Suzuki discloses a system and method wherein the step of storing the symmetric traffic key in a phonebook record associated with the second portable communication device (column 7 lines 31-37).

In reference to claim and 18, Suzuki discloses a system wherein the step of storing a predetermined number of symmetric traffic keys in a cache memory associated with a predetermined number of other portable communication devices in recent communication with the multi-mode portable communication device (column 7 lines 31-37).

In reference to claims 10 and 20, Suzuki establishes a key exchange with a plurality of other predetermine portable communication devices during a background mode (Fig. 16).
Wherein mode 1 corresponds to the idle mode.

Claims 2-3, 9, 11-12, 15, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki in view of Schneier.

In reference to claims 2 and 15, Although Suzuki discloses encrypting the communication between the mobile portable station and the current base station (device that communicates with the portable station), Suzuki does not expressly disclose a system that uses Automatic Public Key Exchange techniques.

Schneier teaches using the public key exchange system using private keys along with a public key of a peer unit before commencing secure communications (page 48).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the public and private keys to perform the key exchange as in Schneier in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because it would make key-exchange easier.

In reference to claim 3, although Suzuki discloses encrypting the communication between the mobile portable station and the current base station (device that communicates with the portable station), Suzuki does not expressly disclose a system that uses Automatic Public Key Exchange is implemented using public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

Schneier discloses a system that uses public-key algorithms for Public Key Exchange techniques (page 48 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the public and private keys to perform the key exchange as in Schneier in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this

because it would make key-exchange easier.

In reference to claims 9 and 19, Suzuki discloses a system wherein the step of establishing a new communication session between the multi-mode portable communication device and the second portable communication device without requiring a new key establishment process (column 3 lines 30-40).

However, Suzuki does not expressly disclose a system that uses Automatic Public Key Exchange techniques.

Schneier teaches using the public key exchange system using private keys along with a public key of a peer unit before commencing secure communications (page 48).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the public and private keys to perform the key exchange as in Schneier in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because it would make key-exchange easier.

In reference to claims 11 and 21, Suzuki discloses a method and system of establishing secure communications among a plurality of portable communication devices, comprising the steps of: storing information associated with a predetermined number of other portable communication devices (column 7 lines 31-37); establishing a symmetric traffic key between a first portable communication device and the predetermined number of other portable communication devices during an idle mode of the first portable communication device (column 5 line 60 to column 6 line 12), wherein the idle mode corresponds to the mode 1 because at this mode no information is being transferred, but the system is ready therefore making this an idle mode; and establishing a secure communication session in a first type of communication

between the first portable communication and at least one among the predetermined number of other portable (Fig 16); switching to at least a second type of communication (column 5 lines 38-45); and sharing the symmetric traffic key between the multi-mode portable communication device and the second portable communication device (column 5 line 60 to column 6 line 12).. Although Suzuki discloses encrypting the communication between the mobile portable station and the current base station (device that communicates with the portable station), Suzuki does not expressly disclose a system that uses Automatic Public Key Exchange is implemented using public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

Schneier discloses a system that uses public-key algorithms for Public Key Exchange techniques (page 48 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the public and private keys to perform the key exchange as in Schneier in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because it would make key-exchange easier.

In reference to claim 12, Suzuki discloses a system wherein the step of establishing a symmetric traffic key comprises contacting the predetermined number of other portable communication devices to determine if their respective keys have expired and performing a background exchange to re-establish a fresh key if the respective key has expired (column 6 lines 55-65).

Claims 4-5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki and Schneier as applied to claim 3 above, and further in view of the article by L-3 Communications.

In reference to claims 4 and 16, although Suzuki discloses encrypting the communication between the mobile portable station and the current base station (device that communicates with the portable station), Suzuki does not expressly disclose a system that uses Automatic Public Key Exchange techniques. Suzuki does not expressly disclose a system wherein the Automatic Public Key exchange is implement by combining public-key algorithms with a signaling scheme such as Future Narrow Band Digital Terminal protocol.

L-3 discloses a terminal that implements the Future Narrow Digital standard and therefore protocol. The protocol includes key management and therefore key exchange (page 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the future narrow band with digital terminal protocol as disclosed by L-3 in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because Future Narrow Band Digital Terminal Protocol does not tie one down to a specific network, but instead assures operation over a variety of narrow band wide band (L-3 page 1).

In reference to claim 5, although Suzuki discloses the switching from one mode to the second mode (column 5 lines 38-55), Suzuki does not disclose the modes comprising interconnect voice, dispatch voice, peer-to peer data, and peer to peer voice

L-3 teaches that FNDT standard defines several modes of operation.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to implement several modes of operation disclosed by L-3 in the system of Suzuki.

One of ordinary skill in the art would have been motivated to do this because vendors are permitted by the FNBDT to incorporate their own enhancements therefore products can meet a set of general requirements (L-3 page 1).

and Whelan
Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki^{as applied} to claim 1 above, and further in view of the FNBDT Signaling Plan.

In reference to claim 6, Suzuki does not disclose a system wherein the step of switching to the second mode from the first mode comprises switching among modes comprising CDMA, TDMA, GSM, and WLAN.

The FNBDT Signaling Plan discloses a system wherein the channels used in the operational mode include digital cellular system.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the future narrow band with digital terminal protocol as disclosed by L-3 in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because Future Narrow Band Digital Terminal Protocol does not tie one down to a specific network, but instead assures operation over a variety of narrow band wide band.

and Whelan
Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki^{as applied} to claim 14 above, and further in view of the FNBDT Signaling Plan and L-3 communications.

In reference to claim 17, although Suzuki discloses the switching from one mode to the second mode of communication (column 5 lines 38-55), Suzuki does not disclose the modes comprising interconnect voice, dispatch voice, peer-to peer data, and peer to peer voice

L-3 teaches that FNDT standard defines several modes of operation.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to implement several modes of operation disclosed by L-3 in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because vendors are permitted by the FNBDT to incorporate their own enhancements therefore products can meet a set of general requirements (L-3 page 1).

Suzuki does not disclose a system wherein the step of switching to the second mode from the first mode comprises switching among modes comprising CDMA, TDMA, GSM, and WLAN.

The FNBDT Signaling Plan discloses a system wherein the channels used in the operational mode include digital cellular system.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the future narrow band with digital terminal protocol as disclosed by L-3 in the system of Suzuki. One of ordinary skill in the art would have been motivated to do this because Future Narrow Band Digital Terminal Protocol does not tie one down to a specific network, but instead assures operation over a variety of narrow band wide band.

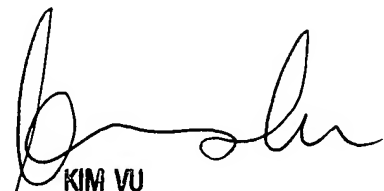
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-38544. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Sunday, February 19, 2006


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100